

**SPAWAR**



*Systems Center*  
**PACIFIC**

TECHNICAL REPORT 3021  
August 2016

# **DITEC Technology Matching Tool (TMT)**

Roger A. Hallman  
Braulio Coronado

Approved for public release

SSC Pacific  
San Diego, CA 92152-5001

**SSC Pacific**  
**San Diego, California 92152-5001**

---

**K. J. Rothenhaus, CAPT, USN**  
**Commanding Officer**

**C. A. Keeney**  
**Executive Director**

**ADMINISTRATIVE INFORMATION**

The work described in this report was performed by the Network Security Engineering Services and Operations Branch (Code 58230) of the Information Assurance Division (Code 58000), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA. This work was funded by the Naval Innovative Science and Engineering (NISE) Program at SSC Pacific.

Released by  
Jose Romero-Mariona, Head  
Network Security Engineering Services  
and Operations Branch

Under authority of  
Elissa J. Huffstetler, Head  
Information Assurance  
Division

This is a work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.

## **EXECUTIVE SUMMARY**

DoD-Centric and Independent Technology Evaluation Capability (DITEC) users may decide that certain capability examinations are less meaningful for them than others. This report introduces a mechanism for allowing security non-experts define their situational needs and be matched with the technology, or suite of technologies, that best satisfy them.

## CONTENTS

EXECUTIVE SUMMARY .....	III
INTRODUCTION .....	1
PROTOTYPING AND IMPLEMENTING THE TMT.....	2
INTEGRATING THE TMT INTO DITEC.....	6
REFERENCES .....	7

## Figures

1. The DITEC TMT leading the user through prioritization of each sub-capability technology vectors, for this demonstration the binary vector for HAIPE technologies.....	2
2. The DITEC TMT showing unprioritized results when the User Requirement vector is the HAIPE technology vector .....	3
3. The DITEC TMT showing unprioritized results when the User Requirement vector is the HAIPE technology vector and only the sub-capability elements which the user affirms are considered.....	4
4. The DITEC TMT showing prioritized results when the User Requirement vector is the HAIPE technology vector .....	5
5. The DITEC TMT showing prioritized results when the User Requirement vector is the HAIPE technology vector and only the sub-capability elements which the user affirms are considered.....	6

## Table

1. DITEC sub-capabilities.....	2
--------------------------------	---

# INTRODUCTION

The United States has been the victim of a number of attacks on both privately held and publicly owned networks (e.g., the Sony Pictures hack which was attributed to North Korea [Sanger and Perlroth, 2014] and the Office of Personnel Management (OPM) breaches which compromised the security of more than 22 million current or former federal employees (Nakashima, 2015). It has been estimated that the United States faces more than 5,000 cyberattacks every hour, and the Pentagon is attacked 10 million times each day (NetStandard, 2014). In light of the growing number and catastrophic results of cyberattacks, cybersecurity has become one of the Department of Defense's (DoD) top priorities. The marketplace of cybersecurity technologies is filled with many different products, all making competing claims of capabilities. Until recently, there has been no uniform system for evaluating cybersecurity products and services.

The Space and Naval Warfare Systems Center Pacific's (SSC Pacific) IA Division has developed the DoD-Centric and Independent Technology Evaluation Capability (DITEC) to streamline cybersecurity technology evaluation. Specifically, DITEC defines a process for evaluating whether or not a product meets DoD needs, security metrics for measuring how well those needs are met, and a framework for comparing various products that address the same cybersecurity technology area (Romero-Mariona, 2014). DITEC evaluates cybersecurity products and services at three levels of granularity: Capability, Sub-Capability, and Sub-Capability Element. There are 10 capabilities, with each capability having a varying number of sub-capabilities and sub-capability elements. There are 44 sub-capabilities and 109 sub-capability elements that are evaluated. DITEC also features an ability that allows individual users to prioritize certain capabilities or sub-capabilities and provide weighted averages that better match the user's needs to technology evaluations (Hallman, Romero-Mariona, Kline; and San Miguel, 2014).

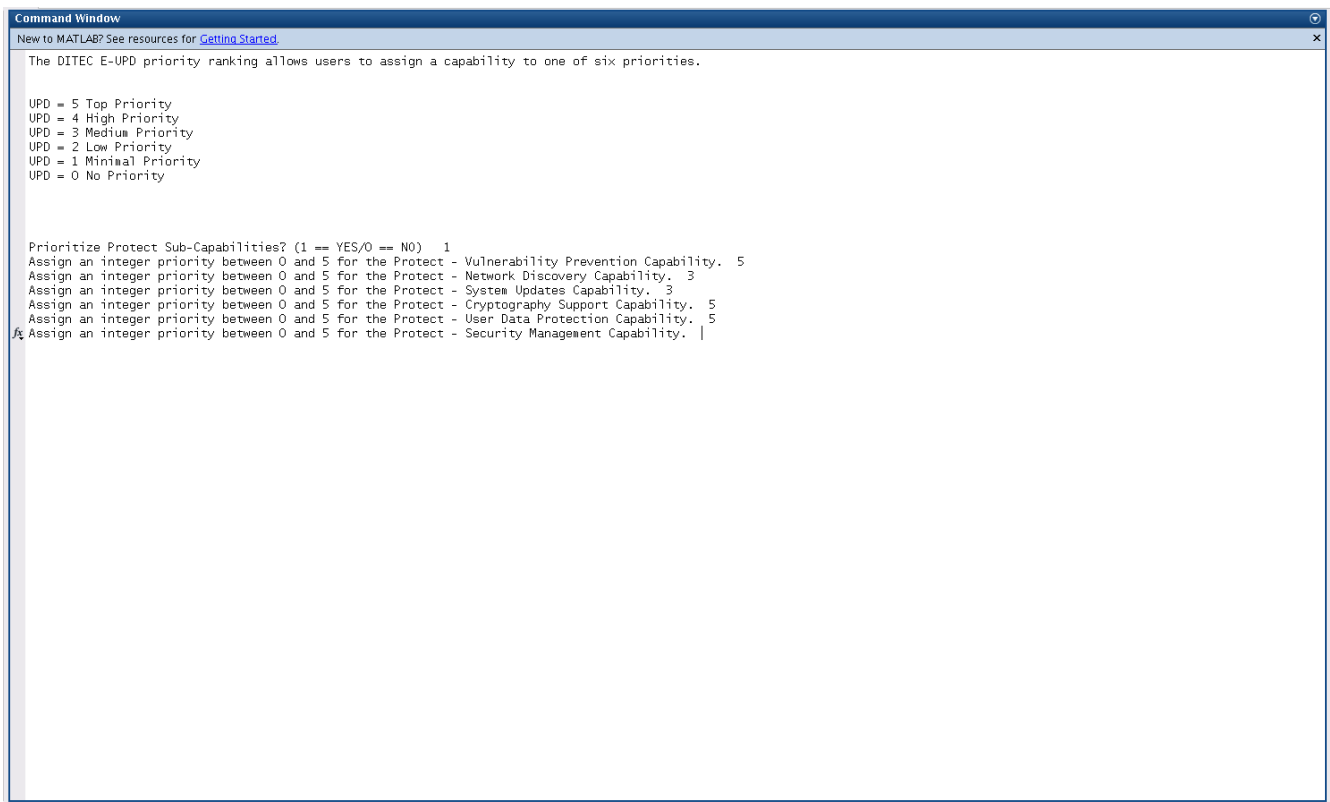
Because of the growth in cybersecurity workforces and a marketplace flooded with diverse technologies, it is expected that cybersecurity professionals may not have great knowledge of all cybersecurity technologies. The DITEC Technology Matching Tool (TMT) was designed to aid technical and acquisition personnel in selecting the appropriate cybersecurity technology to meet their needs. DITEC's Sub-Capability level of granularity is at a level of specificity that can be used to point the user towards certain cybersecurity technologies over others. The TMT leads the user through a series of yes/no questions for each of the 109 sub-capability elements, which gives a binary "User Requirement" vector. The TMT utilizes the User Priority Designation (UPD) scheme described by Hallman et al. (2014) to scale the User Requirement sub-vectors, where the sub-vectors correspond to DITEC's sub-capabilities (Table 1). Each cybersecurity technology is also given a binary vector based on whether or not it performs each sub-capability element. The scaled user requirements vector and each cybersecurity technology vector are then compared with the  $l_2$  norm. The technologies are then matched to the user's requirements, ordered from the least  $l_2$  norm to greatest.

Table 1. DITEC sub-capabilities.

Priority	UPD Rank	Scaling Factor
Top priority	5	1.00
High priority	4	0.85
Medium priority	3	0.55
Low priority	2	0.25
Minimal priority	1	0.10
No priority	0	0.00

## PROTOTYPING AND IMPLEMENTING THE TMT

A prototype of the DITEC TMT was built using MATLAB®. This prototype TMT leads the user through a series of yes/no questions for each of DITEC's 44 sub-capabilities, assigning to each sub-capability a numerical priority. (Figure 1) The User Requirement vectors tested were cybersecurity technology vectors, for this demonstration the binary vector for High Assurance Internet Protocol Encryptor (HAIZE) technologies.



```

Command Window
New to MATLAB? See resources for Getting Started.

The DITEC E-UPD priority ranking allows users to assign a capability to one of six priorities.

UPD = 5 Top Priority
UPD = 4 High Priority
UPD = 3 Medium Priority
UPD = 2 Low Priority
UPD = 1 Minimal Priority
UPD = 0 No Priority

Prioritize Protect Sub-Capabilities? (1 == YES/0 == NO) 1
Assign an integer priority between 0 and 5 for the Protect - Vulnerability Prevention Capability. 5
Assign an integer priority between 0 and 5 for the Protect - Network Discovery Capability. 3
Assign an integer priority between 0 and 5 for the Protect - System Updates Capability. 3
Assign an integer priority between 0 and 5 for the Protect - Cryptography Support Capability. 5
Assign an integer priority between 0 and 5 for the Protect - User Data Protection Capability. 5
Assign an integer priority between 0 and 5 for the Protect - Security Management Capability. |
  
```

Figure 1. The DITEC TMT leading the user through prioritization of each sub-capability technology vectors, for this demonstration the binary vector for HAIZE technologies.

There are two Technology Tables of results currently given by the TMT. The first Technology Table gives the user a simple comparison of the User Requirement vector to each cybersecurity technology vector. (Figure 2) The second Technology Table creates a sub-vector from the cybersecurity technology and User Requirement vectors based on whether an element in the prioritized User Requirement vector is unequal to

zero. If an element in the prioritized User Requirement vector is unequal to zero, then that element and its corresponding element of each cybersecurity technology vector are transferred to a new vector for comparison. That is, the first Technology Table only takes into consideration the sub-capabilities to which the user has assigned a positive UPD Rank or a Sub-Capability Element for which the user has explicitly affirmed a need. (Figure 3).

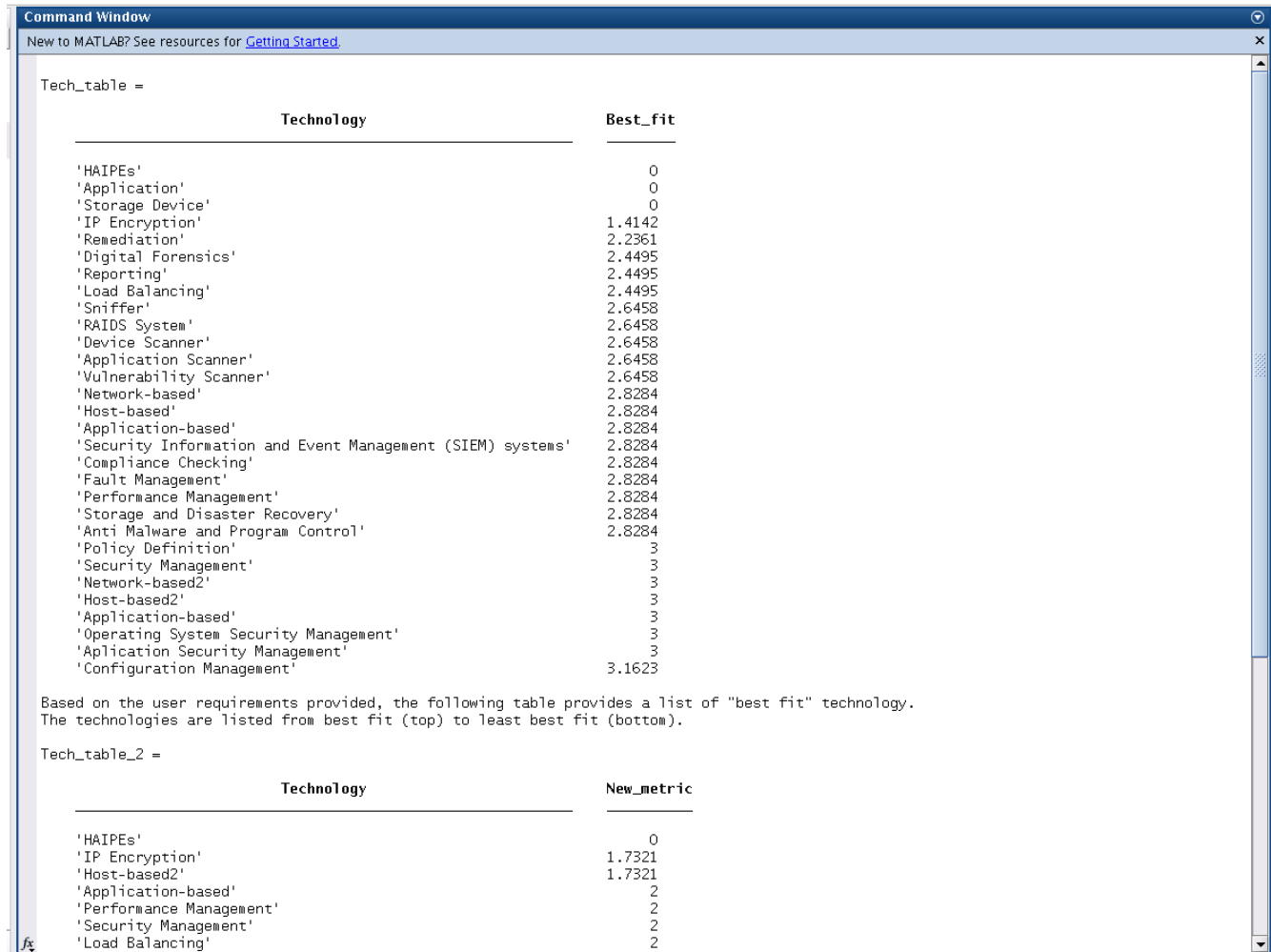


Figure 2. The DITEC TMT showing unprioritized results when the User Requirement vector is the HAIPE technology vector.

Figures 2 and 3 show the difference in TMT Technology Tables when the sub-capability elements are unscaled. (That is, the scaling factor is 1.00.) Figure 2 shows the Technology Table of comparisons to the full User Requirement vector and each cybersecurity technology vector. Figure 3 shows the Technology Table of comparisons when only sub-vector of positively affirmed sub-capability elements of the User Requirement vector and corresponding cybersecurity technology vectors are considered. In this demonstration, the HAIPE technology vector was chosen as the User Requirement vector, and as expected, HAIPE is the top match in both Technology Tables. Note the differences in TMT results further down in the technology tables. In Figure 2, the second, third, and fourth matches are Application Security technologies, Storage Device technologies, and IP Encryption technologies. In Figure 3, on the other hand, the second, third, and fourth matches are IP Encryption technologies, Host-Based Security technologies, and Application-based technologies. Because Technology Table 2 takes into account only those specific capabilities that the user affirms, other capabilities that the user may not be interested in are disregarded and the user is better matched to the cybersecurity technologies meeting their needs.

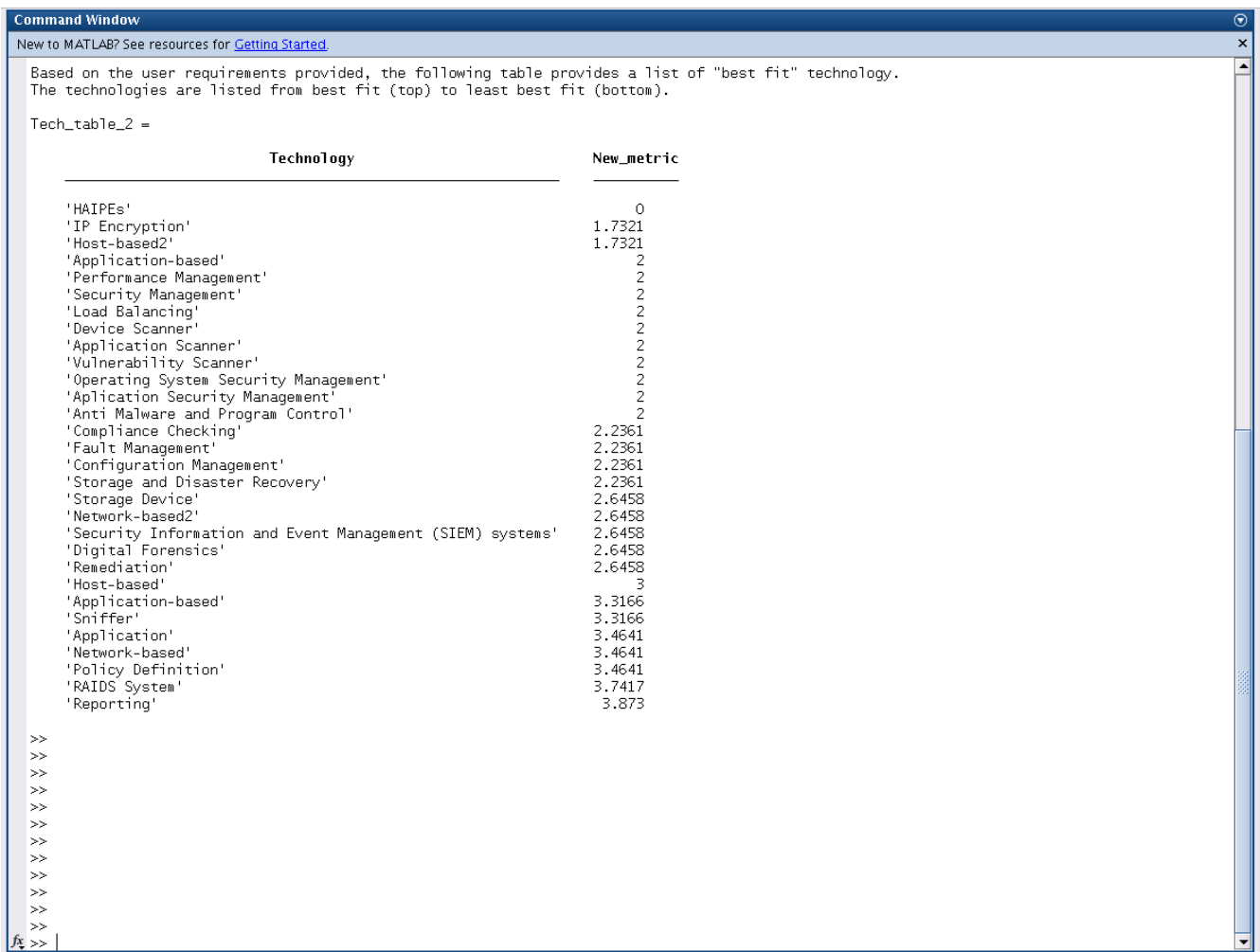


Figure 3. The DITEC TMT showing unprioritized results when the User Requirement vector is the HAIPE technology vector and only the sub-capability elements which the user affirms are considered.

Where Figures 2 and 3 show the unprioritized results, the UPD integrated TMT allows the user <sup>44</sup> prioritizations with which they may better match their unique circumstances to an IA technology. Figure 4 in the current example of the MATLAB<sup>®</sup> prototype shows the TMT Technology Table 1 resulting from one possible priority profile and the same User Requirement vector, while Figure 5 shows the corresponding Technology Table 2. Even with the prioritized scaling, Technology Table 1 gives similar results to the unscaled TMT in Figure 2. Note that with the user priorities scaling the User Requirement vector, the TMT gives slightly different results in the second Technology Table. Even though the User Requirement vector was the HAIPE technology vector, the user's priorities scaled the vector in such a way that a HAIPE may not be the best choice for their needs and priorities. Rather, the user has prioritized sub-capabilities in such a way that Storage Device technologies meet their affirmed capability needs.



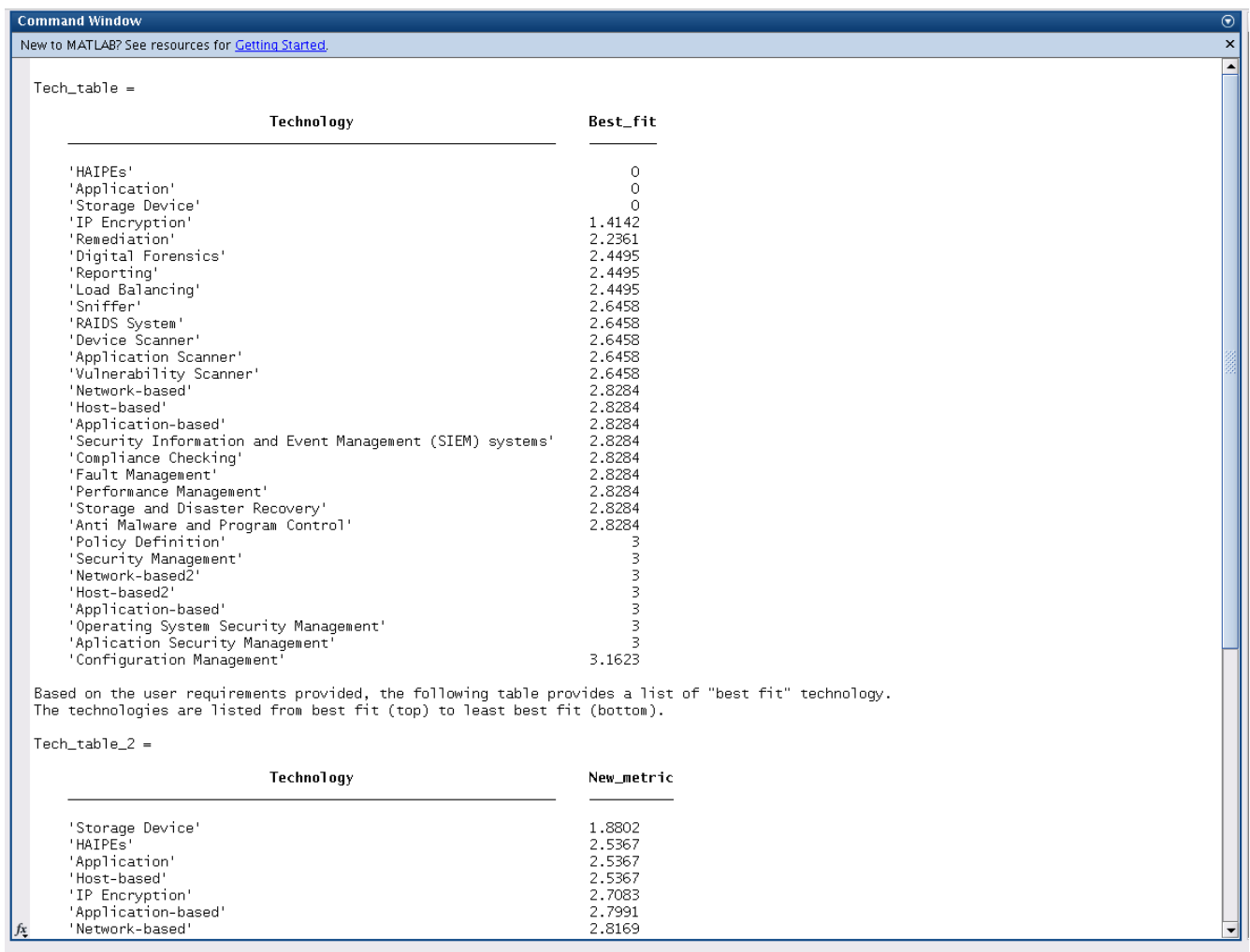


Figure 4. The DITEC TMT showing prioritized results when the User Requirement vector is the HAIP technology vector.

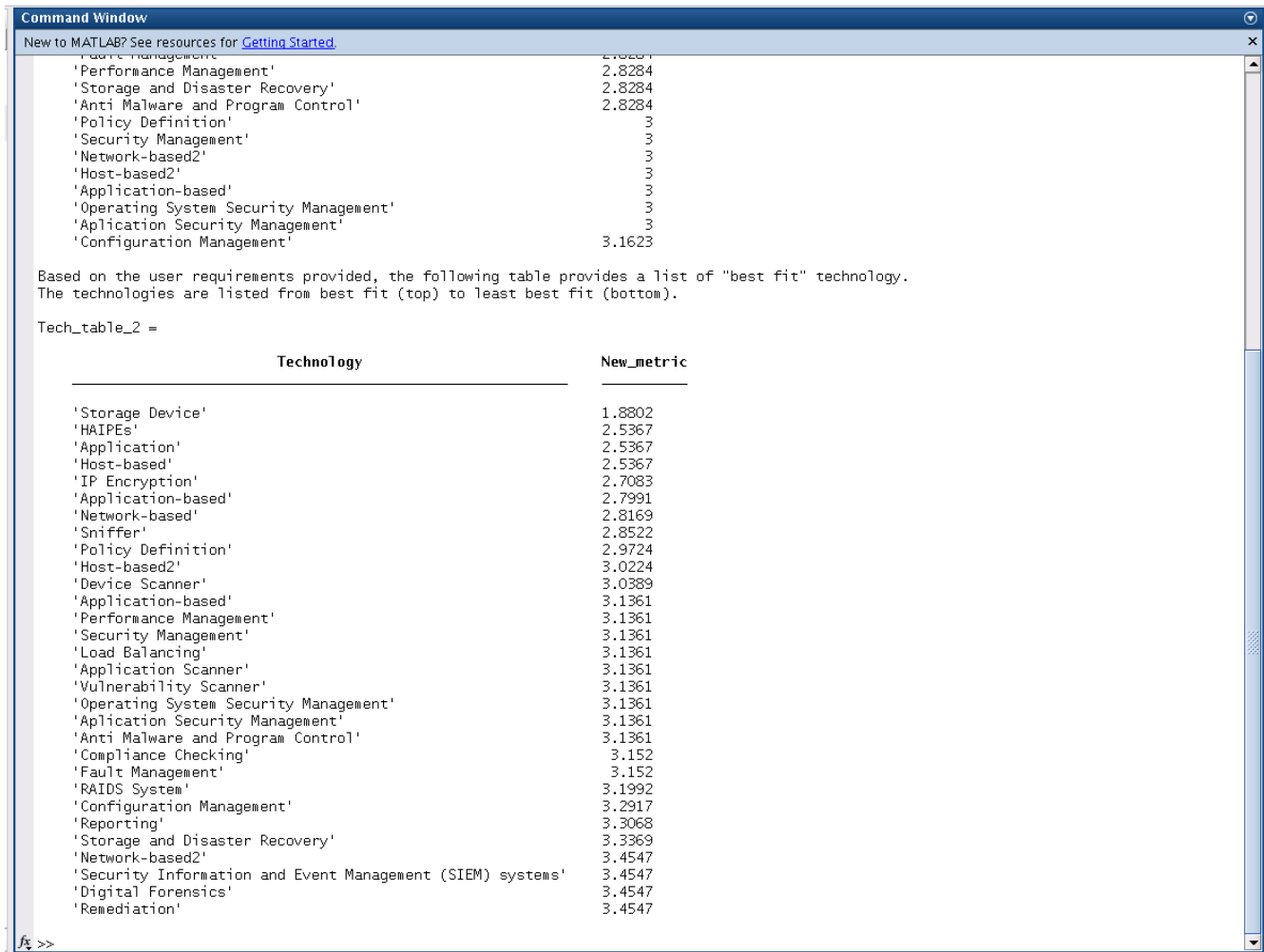


Figure 5. The DITEC TMT showing prioritized results when the User Requirement vector is the HAIPe technology vector and only the sub-capability elements which the user affirms are considered.

## INTEGRATING THE TMT INTO DITEC

The TMT application within DITEC was written in the Python<sup>™</sup> programming language and takes advantage of the Django<sup>®</sup> web application framework. Using Django's form wizard, the user is guided through a series of steps to determine the right technology and suite of technologies to meet their needs. Each step in the tool represents a technological capability and prompts the user to select a rating from 0 to 5 for each of the capability's sub capabilities. These ratings are compared to each technology to determine the "best fit" technologies and technology suites. Django's form wizard is an application that splits forms across multiple web pages. It maintains user data in the back end for processing after the final step in the wizard is completed and provides data validation between steps. The TMT queries the base capability table and generates a form for each capability. Each form is composed of a title with capability information and a list of fields which represent the sub capabilities associated to the capability. Each field is composed of a label for the sub capability, a slider and an integer box. The user can select a rating for the slider by dragging the slider bar from 0 to 5. The integer box will update when the slider value is changed and vice-versa.

A back button is provided which will take the user back to the previous step. A next button is provided which will validate the users ratings before continuing to the next step. Finally, a skip button is provided which will set the rating for each field to 0 and continue to the next step. Currently, the TMT wizard displays steps with fields at the sub capability level. However, the data maintained in the wizard is at the sub capability element level. User ratings are simply passed down from sub-capability to sub-capability element. Data is stored in the form of a dictionary with sub-capability elements as the key and the users' ratings as the value and is maintained in a session on a per-site-visitor basis. Tooltips are provided when the user hovers the mouse over a capability, sub-capability, or technology item in the user interface. A tool tip is tied to the description column in the corresponding items table. The order of the steps in the wizard is determined by the TMT sort order column in the base Capability table.

## REFERENCES

- Sanger, D.; N. Perlroth. 2014. "US Said to Find North Korea Ordered Attack on Sony," *New York Times*, (December 17). Available online at <http://nyti.ms/1Ae7n9r>.
- Nakashima, E. 2015. "Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say," *Washington Post* (July 9). Available online at <http://www.washingtonpost.com/blogs/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/>. Accessed August 11, 2016.
- NetStandard. 2014. "US Hit with More Than 5,000 Attacks Every Hour." July 7. Available online at <http://www.netstandard.com/cyberattacks-map/>. Accessed August 11, 2016.
- Romero-Mariona, J. 2014. "DITEC (DoD-Centric and Independent Technology Evaluation Capability): A Process for Testing Security." IEEE Seventh International Conference on Software Testing, Verification and Validation Workshops (ICSTW). March 31 – April 4, Cleveland, OH.
- Hallman, R.; J. Romero-Mariona, M. Kline, and J. San Miguel. 2014. "DITEC User Priority Designation (UPD) Algorithm: An Approach to Prioritizing Technology Evaluations." Technical Document 3288. Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA. Available online at <http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA619280>. Accessed August 11, 2016.

<b>REPORT DOCUMENTATION PAGE</b>				<i>Form Approved</i> OMB No. 0704-01-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden to Department of Defense, Washington Headquarters Services Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>					
<b>1. REPORT DATE (DD-MM-YYYY)</b> August 2016		<b>2. REPORT TYPE</b> Final		<b>3. DATES COVERED (From - To)</b>	
<b>4. TITLE AND SUBTITLE</b>  DITEC Technology Matching Tool (TMT)				<b>5a. CONTRACT NUMBER</b>	
				<b>5b. GRANT NUMBER</b>	
				<b>5c. PROGRAM ELEMENT NUMBER</b>	
<b>6. AUTHORS</b>  Roger Hallman Braulio Coronado				<b>5d. PROJECT NUMBER</b>	
				<b>5e. TASK NUMBER</b>	
				<b>5f. WORK UNIT NUMBER</b>	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> SSC Pacific 53560 Hull Street San Diego, CA 92152-5001				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>  TR 3021	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> SSC Pacific Naval Innovative Science and Engineering (NISE) Program 53560 Hull Street San Diego, CA 92152-5001				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b> DITEC, TMT	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b>	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b>  Approved for public release.					
<b>13. SUPPLEMENTARY NOTES</b>  This is work of the United States Government and therefore is not copyrighted. This work may be copied and disseminated without restriction.					
<b>14. ABSTRACT</b>  DoD-Centric and Independent Technology Evaluation Capability (DITEC) users may decide that certain capability examinations are less meaningful for them than others. This report introduces a mechanism for allowing security non-experts define their situational needs and be matched with the technology, or suite of technologies, that best satisfy them.					
<b>15. SUBJECT TERMS</b>  cybersecurity; DoD-centric and Independent Technology Evaluation Capability (DITEC); technology matching tool; user priority designation scheme; prototyping; High Assurance Internet Protocol Encryptor (HAIRPE)					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			Roger A. Hallman
U	U	U	U	14	<b>19b. TELEPHONE NUMBER (Include area code)</b> 619-553-7905

## INITIAL DISTRIBUTION

84300	Library	(1)
85300	Archive/Stock	(1)
58230	R. Hallman	(1)
53624	B. Coronado	(1)

Defense Technical Information Center Fort Belvoir, VA 22060-6218	(1)
---	-----

Approved for public release.



SSC Pacific  
San Diego, CA 92152-5001